FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1639656-000

Total Deleted Page(s) = 273
Page 5 ~ Duplicate - Serial 8;
Page 6 ~ Duplicate - Serial 8;
Page 7 ~ Duplicate - Serial 8;
Page 8 ~ b6; b7C;
Page 9 ~ b6; b7C;
Page 14 ~ Duplicate - Serial 19;
Page 15 ~ Duplicate - Serial 19;
Page 16 ~ Duplicate - Serial 19;
Page 17 ~ Duplicate - Serial 19;
Page 30 ~ Referral/Direct;
Page 31 ~ Referral/Direct;
Page 32 ~ Referral/Direct;
Page 33 ~ Referral/Direct;
Page 34 ~ Referral/Direct;
Page 35 ~ Referral/Direct;
Page 36 ~ Referral/Direct;
Page 37 ~ Referral/Direct;
Page 38 ~ Referral/Direct;
Page 39 ~ Referral/Direct;
Page 40 ~ Referral/Direct;
Page 41 ~ Referral/Direct;
Page 42 ~ Referral/Direct;
Page 43 ~ Referral/Direct;
Page 44 ~ Referral/Direct;
Page 45 ~ Referral/Direct;
Page 46 ~ Referral/Direct;
Page 47 ~ Referral/Direct;
Page 48 ~ Referral/Direct;
Page 49 ~ Referral/Direct;
Page 50 ~ Referral/Direct;
Page 51 ~ Referral/Direct;
Page 52 ~ Referral/Direct;
Page 53 ~ Referral/Direct;
Page 54 ~ Referral/Direct;
Page 55 ~ Referral/Direct;
Page 56 ~ Referral/Direct;
Page 57 ~ Referral/Direct;
Page 58 ~ Referral/Direct;
Page 59 ~ Referral/Direct;
Page 60 ~ Referral/Direct;
Page 61 ~ Referral/Direct;
Page 62 ~ Referral/Direct;
Page 63 ~ Referral/Direct;
Page 64 ~ Referral/Direct;
Page 65 ~ Referral/Direct;
Page 66 ~ Referral/Direct;
Page 67 ~ Referral/Direct;
Page 68 ~ Referral/Direct;
Page 69 ~ Referral/Direct;
Page 70 ~ Referral/Direct;
Page 71 ~ Referral/Direct;
Page 72 ~ Referral/Direct;
Page 73 ~ Referral/Direct;
Page 74 ~ Referral/Direct;
Page 75 ~ Referral/Direct;
Page 76 ~ Referral/Direct;
Page 77 ~ Referral/Direct;
Page 78 ~ Referral/Direct;
Page 79 ~ Referral/Direct;
Page 80 ~ Referral/Direct;
Page 81 ~ Referral/Direct;
Page 82 ~ Referral/Direct;
Page 83 ~ Referral/Direct;
Page 84 ~ Referral/Direct;
Page 85 ~ Referral/Direct;
Page 86 ~ Referral/Direct;
Page 87 ~ Referral/Direct;

(12/31/1995)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-21-2012 BY [redacted]

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 03/04/1998

To: FBI Headquarters **Attn:** NSD/CID/CITAC
SSA [redacted]

From: Boston
Squad C-11
Contact: SA [redacted]

b6
b7C

Approved By: [redacted]

Drafted By: [redacted]:tad

Case ID #: 288-HQ-1242560-165 (Pending)

Title: Operation Solar Sunrise

Synopsis: [redacted] reinterviewed, complete copy of [redacted] home directory obtained, selected files from [redacted] home directory obtained.

b6
b7C

Reference: 288-HQ-1242560 Serial 81

Enclosures: Enclosed for Headquarters is one FD-302 from [redacted] one FD-302 from [redacted] one FD-302 from [redacted] with the [redacted] of [redacted] one [redacted] with selected files from [redacted] and files from [redacted] and the original interview notes of [redacted]

b6
b7C
b7E

Details: See attached FD-302 of [redacted]

♦♦

Page 161 ~ Referral/Direct;
Page 162 ~ Referral/Direct;
Page 163 ~ Referral/Direct;
Page 164 ~ Referral/Direct;
Page 165 ~ Referral/Direct;
Page 166 ~ Referral/Direct;
Page 167 ~ Referral/Direct;
Page 168 ~ Referral/Direct;
Page 169 ~ Referral/Direct;
Page 170 ~ Referral/Direct;
Page 171 ~ Referral/Direct;
Page 172 ~ Referral/Direct;
Page 173 ~ Referral/Direct;
Page 174 ~ Referral/Direct;
Page 175 ~ Referral/Direct;
Page 176 ~ Referral/Direct;
Page 177 ~ Referral/Direct;
Page 178 ~ Referral/Direct;
Page 179 ~ Referral/Direct;
Page 180 ~ Referral/Direct;
Page 181 ~ Referral/Direct;
Page 182 ~ Referral/Direct;
Page 183 ~ Referral/Direct;
Page 184 ~ Referral/Direct;
Page 185 ~ Referral/Direct;
Page 186 ~ Referral/Direct;
Page 187 ~ Referral/Direct;
Page 188 ~ Referral/Direct;
Page 189 ~ Referral/Direct;
Page 190 ~ Referral/Direct;
Page 191 ~ Referral/Direct;
Page 192 ~ Referral/Direct;
Page 193 ~ Referral/Direct;
Page 194 ~ Referral/Direct;
Page 195 ~ Referral/Direct;
Page 196 ~ Referral/Direct;
Page 197 ~ Referral/Direct;
Page 198 ~ Referral/Direct;
Page 199 ~ Referral/Direct;
Page 200 ~ Referral/Direct;
Page 201 ~ Referral/Direct;
Page 202 ~ Referral/Direct;
Page 203 ~ Referral/Direct;
Page 204 ~ Referral/Direct;
Page 205 ~ Referral/Direct;
Page 206 ~ Referral/Direct;
Page 207 ~ Referral/Direct;
Page 208 ~ Referral/Direct;
Page 209 ~ Referral/Direct;
Page 210 ~ Referral/Direct;
Page 211 ~ Referral/Direct;
Page 212 ~ Referral/Direct;
Page 213 ~ Referral/Direct;
Page 214 ~ Referral/Direct;
Page 215 ~ Referral/Direct;
Page 216 ~ Referral/Direct;
Page 217 ~ Referral/Direct;
Page 218 ~ Referral/Direct;
Page 220 ~ Referral/Consult;
Page 221 ~ Referral/Consult;
Page 224 ~ Referral/Consult;
Page 229 ~ b6; b7C;
Page 230 ~ b6; b7C;
Page 231 ~ b6; b7C;
Page 232 ~ b6; b7C;
Page 233 ~ b6; b7C;
Page 234 ~ b6; b7C;
Page 235 ~ b6; b7C;
Page 236 ~ b6; b7C;
Page 237 ~ Duplicate - Serial 139;
Page 238 ~ b6; b7C;
Page 239 ~ b6; b7C;
Page 240 ~ b6; b7C;

Page 241 ~ b6; b7C;
Page 242 ~ b6; b7C;
Page 243 ~ b6; b7C;
Page 244 ~ b6; b7C;
Page 245 ~ b6; b7C;
Page 246 ~ b6; b7C;
Page 247 ~ b6; b7C;
Page 248 ~ b6; b7C;
Page 249 ~ b6; b7C;
Page 250 ~ b3; b6; b7C; OTHER;
Page 251 ~ b3; b6; b7C; OTHER;
Page 252 ~ b3; b6; b7C; OTHER;
Page 256 ~ Referral/Consult;
Page 257 ~ Referral/Consult;
Page 258 ~ Referral/Consult;
Page 259 ~ Referral/Consult;
Page 260 ~ Referral/Consult;
Page 261 ~ Referral/Consult;
Page 266 ~ b6; b7C;
Page 267 ~ b6; b7C;
Page 268 ~ b6; b7C; b7E;
Page 269 ~ b6; b7C; b7E;
Page 270 ~ b6; b7C; b7E;
Page 271 ~ b6; b7C; b7E;
Page 272 ~ b6; b7C; b7E;
Page 273 ~ b6; b7C; b7E;
Page 274 ~ b6; b7C; b7E;
Page 275 ~ b6; b7C; b7E;
Page 277 ~ b6; b7C; b7E;
Page 278 ~ b6; b7C; b7E;
Page 279 ~ b6; b7C; b7E;
Page 280 ~ b6; b7C; b7E;
Page 281 ~ b6; b7C; b7E;
Page 282 ~ b6; b7C; b7E;
Page 283 ~ b6; b7C; b7E;
Page 284 ~ b6; b7C; b7E;
Page 285 ~ b6; b7C; b7E;
Page 286 ~ b6; b7C; b7E;
Page 287 ~ b6; b7C; b7E;
Page 288 ~ b6; b7C; b7E;
Page 289 ~ b6; b7C; b7E;
Page 290 ~ b6; b7C; b7E;
Page 291 ~ b6; b7C; b7E;
Page 292 ~ b6; b7C; b7E;
Page 293 ~ b6; b7C; b7E;
Page 294 ~ b7E;
Page 295 ~ b6; b7C; b7E;
Page 296 ~ b6; b7C; b7E;
Page 297 ~ b7E;
Page 303 ~ b6; b7C; b7E;
Page 304 ~ b6; b7C; b7E;
Page 305 ~ b6; b7C; b7E;
Page 306 ~ b6; b7C; b7E;
Page 307 ~ b6; b7C; b7E;
Page 308 ~ b6; b7C; b7E;
Page 313 ~ Duplicate - Serial 84;
Page 314 ~ Duplicate - Serial 84;
Page 315 ~ Duplicate - Serial 84;
Page 318 ~ b6; b7C; b7E;
Page 319 ~ b6; b7C; b7E;

XXXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXXX

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-20-2012 BY [redacted]

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 2/11/98

[redacted] Office of General Counsel, PSINET, 510 Huntmare Park Pl., Herndon, Virginia, 22070, phone: [redacted] being aware of the identity of the interviewing agent, received service of the attached court order.

[redacted]

A copy of this signed order was faxed to [redacted] on 2/11/98.

b3
b6
b7C
OTHER Sealed pursuant to court order

(1)
SD

Investigation on 2/11/98 at Fairfax, VA (telephonically)

File # 288-HQ-1242560 -85 Date dictated 2/11/98

by SA [redacted]

l/c 5731

SERIALIZED FILED
FEB 11 1998
FBI - WASH. METRO FIELD OFFICE

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-20-2012 BY [redacted]

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 2/11/98

[redacted] mailing address: [redacted] phone: [redacted] was advised of the identity of the interviewing agent, and received service of the attached court order in his [redacted] office located at [redacted]

[redacted] stated [redacted] would be advised of the court order and would oversee the technical implementation of the trap and trace.

(1)
TJ mm

b3
b6
b7C
OTHER Sealed pursuant to court order

Investigation on 2/11/98 at Fairfax, Virginia

File # 288-HQ-1242560-SU Date dictated N/A

by SA [redacted]
5737

SERIALIZED JCM INDEXED
FILED JCM
FEB 12 1998
FBI - WASH. METRO FIELD OFFICE

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency;

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-20-2012 BY [redacted]

Automated Serial Permanent Charge-Out
FD-5a (1-5-94)

Date: 02/19/98 Time: 14:09

Case ID: 288-HQ-1242560 Serial: 88

Description of Document:

Type : EC
Date : 02/18/98
To : NSD/CID
From : KNOXVILLE
Topic: (U) TO RESPOND TO LEADS CONCERNING CAPTIONED MATTER.

Reason for Permanent Charge-Out:

CHANGE MADE TO DOCUMENT

Employee: [redacted] b6 b7C

288-HQ-1242560-88

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-20-2012 BY [redacted]

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 2/12/98

[redacted] mailing address: [redacted]
[redacted] phone: [redacted]
was advised of the identitities of the interviewing agents, and received service of the attached court order in his [redacted] office located at [redacted]

[redacted]

[redacted] stated [redacted] would be advised of the court order and would oversee the technical implementation of the trap and trace.

(1)

b3
b6
b7C
OTHER Sealed pursuant to court order

Investigation on 2/12/98 at Fairfax, Virginia

File # 288-HQ-1242560-89

by SA [redacted]
SA [redacted]

Date dictated N/A

SEARCHED INDEXED SERIALIZED FILED
FEB 12 1998
FBI - WASH. METRO FIELD OFFICE

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FD-302 (Rev. 10-6-95)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-20-2012 BY [redacted]

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 2/12/98

[redacted]
being aware of the identity of the interviewing agent, received service of the attached court order.

[redacted]

[redacted] A copy of this signed order was delivered in person to on 2/12/98.

b3
b6
b7C
OTHER Sealed pursuant to court order

Investigation on 2/12/98 at Washington, DC

File # 288-HQ-1242560-90 Date dictated 2/12/98

by SA [redacted]

UNSEALED FILED
FEB 12 1998
FBI/DOJ
METRO FIELD OFFICE

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

57/56

(01/26/1998)

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-20-2012 BY [redacted]

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY **Date:** 02/18/1998

To: NSD/CID **Attn:** CITAC, SSA [redacted]
ROOM 11887

From: Knoxville
Squad 4
Contact: SA [redacted]

b6
b7C

DEPTown.
Approved By: [redacted]

Drafted By: [redacted] :amc 96

Case ID #: (U) ~~(S)~~ 288-HQ-1242560 (Pending)

Title: (U) ~~(S)~~ SOLAR SUNRISE;
CITA MATTERS

Synopsis: (U) To respond to leads concerning captioned matter.

(U) ~~(S)~~ ~~**Classified By: 4511, CITAC/D5**~~
~~**Reason : 1.5(c)**~~
~~**Declassify On: 02/12/2008**~~

Administrative: (U) ~~(S)~~ Referenced communication to all field offices, captioned as above, dated 2/12/1998. Referral/Consult

~~SECRET~~

049AMC01.ECF

To: NSD/CID From: Knoxville
Re: (U) ~~(S)~~ 288-HQ-1242560, 02/18/1998

Referral/Consult

♦♦

(12/31/1995)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-20-2012 BY [redacted]

454

FEDERAL BUREAU OF INVESTIGATION

Precedence: IMMEDIATE **Date:** 02/18/1998

To: All Field Offices **Attn:** PERSONAL ATTENTION:
Media Coordinator
CITA Supervisor

From: National Security Division
CITAC
Contact: [redacted]

Approved By: [redacted] b6
Geide Kenneth M b7C

Drafted By: [redacted] :mjw

Case ID #: 288-HQ-1242560-97 (Pending)

Title: SOLAR SUNRISE
COMPUTER INTRUSION

Synopsis: Advisory re press interest in investigation

Details: SOLAR SUNRISE is a pending investigation managed out of FBIHQ/CITAC with related cases in numerous field offices. The case involves a relatively large number of related computer intrusions into unclassified military computer systems. The scale and timing of these intrusions, which continue to occur as the United States prepares for major military operations, have raised major concerns for the Department of Defense.

From its early stages, the investigation has been classified at the secret level. Nevertheless, on 2-13-98, a fairly detailed report appeared in a technical publication. The DOD press office, FBIHQ, and at least one FBI field office subsequently received inquiries from the press. FBIHQ anticipates that there will be continued interest in this matter by the national press.

Until further notice, any and all press inquiries should be referred, without further comment, to SSA [redacted] b6
[redacted] Office of Public and Congressional Affairs [redacted] b7C

Due to the sensitivity of the investigation, all field offices should observe appropriate measures to prevent unauthorized dissemination of information. In particular, offices should be vigilant about giving any information to persons who claim to be representing DOD or other agencies involved in the investigation. The identity and affiliation of any such person should be verified prior to communicating any information. Secure telephones should be used for any outside communications relating to this investigation.

To: All Field Offices From: National Security Division
Re: 288-HQ-1242560, 02/18/1998

CC: [redacted] OPCA b6 b7C

♦♦

(03/31/95)

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-20-2012 BY [redacted]

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE Date: 2/18/1998

To: Director, FBI Attn: Acting Unit Chief
[redacted]

From: WFO
C-17/NVRA
Contact: SSA [redacted] b6 b7C

Approved By: [redacted]

Drafted By: [redacted] :rar

File Number(s): 288-HQ-1242560 98 (Pending)

Title: SOLAR SUNRISE;
CITAC MATTERS;
OO: HQ

Synopsis: Following is the status of WFO's involvement in this investigation.

Reference: EC dated 2/17/98 to Houston Division.

Details:

[redacted] U.S. NAVY - VICTIM; OO: WFO".

SA [redacted] is coordinating all investigative activity with Agents of the Naval Criminal Investigative Service (NCIS) based in both Washington, D.C. and Jacksonville, Florida. Evidence obtained from subject's University of Northern Florida (UNF) account has disclosed continuing access to that account from an IBM.NET connection. A request was submitted today to DOJ for a pen register to require [redacted] to [redacted] Results of the pen are anticipated to support a subsequent 2703 (d) order to [redacted] for [redacted] The subject's current whereabouts and employment are known. Coordination with the NCIS Agents will continue. The installation of the monitoring software at [redacted] was initiated [redacted] by [redacted] b3 b6 b7C b7E

[redacted]

288-HQ-1242560 "SOLAR SUNRISE: CITAC MATTERS: OO: HQ"

[redacted] b6 b7C

(03/31/95)

FEDERAL BUREAU OF INVESTIGATION

To: WMFO From: WMFO
Re: 66-, 12/01/1995

Optical disks received from Houston and copies will be made ASAP for AF, Navy, DISA, and [redacted] Contact has been made with IBM network management and IBM is trace routing Israeli network leg. Should know by tomorrow monitoring ability from within US of overseas leased nets. Referral/Consult

Analysis performed for three compromised systems: (1) Univ. California, Berkeley, (2) Andrews AFB, (3) US Naval Academy. To date, nothing significant has been identified in the most recent JID data collected for the past day or so. Observed two suspicious sites (netgate.saes.com and netdex.com). WFO has not confirmed the nexus on these sites.

Gospelcom.net not contacted due to NCIC checks revealing [redacted] Thegospel.com does not answer phone, nor do they call back when message left. Will continue to try to contact. Slip-stream.net SYSOP did not see anything unusual. They have been hacked before and do not consider this out of the norm. b6 b7C

Referral/Consult

On 02/13/98, Court Order served on [redacted] WFO CART tasked to make copies for Navy, AF, [redacted] and DISA. Limited data analysis has been conducted due to time constraints. [redacted]

[redacted] WFO cannot look through these files and is awaiting DOJ advice. WFO obtaining from UM copies of their computer policy that the students are informed of when their receive their computer accounts. WFO does not believe that the student, [redacted] should be contacted to give consent due to the nature of the case and the fact that the student is a [redacted]

Referral/Consult

[redacted] **VICTIM; OO: WFO"**

b3
b6
b7C
b7E
OTHER Sealed pursuant to court order

(03/31/95)

FEDERAL BUREAU OF INVESTIGATION

To: WMFO From: WMFO
Re: 66-, 12/01/1995

SA [redacted] is addressing this matter with the assistance of the [redacted] and WFO CART. Subject's home was consensually searched for computer and computer media the evening of 2/17/98. Newark Division CART [redacted] Copy will be provided to [redacted] ASAP. Subject provided detailed interview to both FBI and [redacted] Agents. Gave no indication he was part of ongoing investigation 288-HQ-1242560. A review of his system is under way.

b6
b7C
b7E
Referral/Consult

(03/31/95)

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-20-2012 BY [redacted]

439

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE Date: 2/19/1998

To: Director, FBI Attn: Acting Unit Chief
[redacted]

From: WFO
C-17/NVRA
Contact: SSA [redacted] b6 b7C

Approved By: [redacted]

Drafted By: [redacted]:rar

File Number(s): 288-HQ-1242560 99 (Pending)

Title: SOLAR SUNRISE;
CITAC MATTERS;
OO: HQ

Synopsis: Following is the status of WFO's involvement in this investigation as of 2/19/98.

Reference: EC dated 2/17/98 to Houston Division.

Details:

[redacted] U.S. NAVY - VICTIM; OO: WFO".

SA [redacted] is coordinating all investigative activity with Agents of the Naval Criminal Investigative Service (NCIS) based in both Washington, D.C. and Jacksonville, Florida. Evidence obtained from subject's University of Northern Florida (UNF) account has disclosed continuing access to that account from an IBM.NET connection. The Trap & Trace/pen register order for [redacted] is being submitted this evening to the magistrate. Order requires [redacted] Results are anticipated to support a subsequent 2703 (d) order to [redacted] for [redacted] The subject's current whereabouts and employment are known. Coordination with the NCIS Agents will continue. The installation of the monitoring software at [redacted] was initiated [redacted] by [redacted] WFO is contacting Georgetown University, University of Virginia, and

b3 b6 b7C b7E

FEDERAL BUREAU OF INVESTIGATION

To: WMFO From: WMFO
Re: 66-, 12/01/1995

Georgia State University, and the original ISP victim/complainant in Lawton, OK.

288-HQ-1242560 "SOLAR SUNRISE: CITAC MATTERS: OO: HQ"

Optical disks received from Houston. Copies will be made ASAP for AF, Navy, DISA, and [redacted] Contact has been made with IBM network management and IBM is trace routing Israeli network leg. Should know soon of monitoring ability from within US of overseas leased nets. Referral/Consult

Analysis performed for three compromised systems: (1) Univ. California, Berkeley, (2) Andrews AFB, (3) US Naval Academy. To date, nothing significant has been identified in the most recent JID data collected for the past day or so. Observed two suspicious sites (netgate.saes.com and netdex.com). WFO has not confirmed the nexus on these sites.

Gospelcom.net not contacted due to NCIC checks revealing [redacted] Thegospel.com does not answer phone, nor do they call back when message left. Will continue to try to contact. Slip-stream.net SYSOP did not see anything unusual. They have been hacked before and do not consider this out of the norm b6 b7C b3

OTHER Sealed pursuant to court order

On 02/13/98, Court Order served on [redacted] Second 2703 (b) order provided to [redacted] Second order will provide additional information.

FERMI Labs and Oakridge National Labs report no intrusions at their sites. All traffic to/from labs is legitimate and explainable. No known connection to this case.

No further information from DISA.

[redacted] VICTIM; OO: WFO"

SA [redacted] is addressing this matter with the assistance of the [redacted] and WFO CART. Subject's home was consensually searched for computer and computer media the evening of 2/17/98. Newark Division CART [redacted] Copy will be provided

b3
b6
b7C
b7E
Referral/Consult

(03/31/95)

FEDERAL BUREAU OF INVESTIGATION

To: WMFO From: WMFO
Re: 66-, 12/01/1995 Referral/Consult

to [redacted] ASAP. Subject provided detailed interview to both FBI and [redacted] Agents. Gave no indication he was part of ongoing investigation 288-HQ-1242560. A review of his system is under way.

(12/31/1995)

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-25-2012 BY [redacted]

439

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY **Date:** 02/22/1998

To: San Francisco **Attn:** SSA [redacted]
SA [redacted]

From: CID/NSA
CITAC/CIU/ Rm 11887
Contact: [redacted]

Approved By: Geide Kenenth M KG/AKL
[redacted] AKL

b6
b7C
b7E

Drafted By: [redacted]:heg

Case ID #: 288-HQ-1242560-102 (Pending)
[redacted] (Pending)

Title: Solar Sunrise;
CITA Matters;
OO:HQ

Synopsis: To request results of T-III and [redacted]

b3

Details: The computer crimes section of the Department of Justice will be hosting a meeting on Monday, Feb 23 at 2:00PM EST. Purpose of the meeting will be to review the results of ongoing investigations at San Francisco, Houston, and Washington field offices to allow a determination as to prosecutive initiatives to be taken. It will therefore be necessary for CITAC personnel attending this meeting to have all current results of investigation.

Uploaded by [illegible]

To: San Francisco From: CID/NSA
Re: 288-HQ-1242560, 02/22/1998

LEAD (s):

Set Lead 1:

SAN FRANCISCO

AT SAN FRANCISCO

Will provide to CITAC, by Monday Feb 23 at 10:30 AM EST, the results of T-III and [redacted] b3

♦♦

FD-448 (Rev. 2-16-95)

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-20-2012 BY [redacted]

439

FBI FACSIMILE

COVERSHEET

PRECEDENCE

- [X] Immediate
- [ ] Priority
- [ ] Routine

CLASSIFICATION

- [ ] Top Secret
- [X] ~~Secret~~
- [ ] Confidential
- [ ] Sensitive
- [ ] Unclassified

Time Transmitted: _____
Sender's Initials: MJW
Number of Pages: 3
(including coversheet)

To: [redacted]/OGC
Name of Office

Date: 2/20/98

Facsimile Number: [redacted] Referral/Consult

Attn: [redacted]
Name Room Telephone

From: OGC/NSLU
Name of Office

Subject: Detailee Request Letter

Special Handling Instructions: _____

Originator's Name: [redacted] Telephone: [redacted] b6 b7C

Originator's Facsimile Number: [redacted]

Approved: MJW

288-HQ-1242560-129

Brief Description of Communication Faxed: Request Letter, per our discussion

Call me, or page me at [redacted] (if I don't answer my phone)

288-HQ-1242560

FD-448 (Rev. 2-16-95)

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-20-2012 BY [redacted]

1/39

FBI FACSIMILE

COVERSHEET

PRECEDENCE

- [X] Immediate
- [ ] Priority
- [ ] Routine

CLASSIFICATION

- [ ] Top Secret
- [ ] Secret
- [ ] Confidential
- [ ] Sensitive
- [X] Unclassified

Time Transmitted: _____
Sender's Initials: MJW
Number of Pages: 2
(including coversheet)

To: [redacted] _____ Date: 2/20/98
Name of Office

Facsimile Number: [redacted]

Attn: [redacted] Referral/Consult
Name Room Telephone

From: FBI/OGC
Name of Office

Subject: Detail Request Letter
288-HQ-1242520

Special Handling Instructions: _____

Originator's Name: [redacted] Telephone: [redacted] b6 b7C

Originator's Facsimile Number: _____

Approved: MJW

288-HQ-1242520-130

Brief Description of Communication Faxed: Per my telephone conversation

with [redacted] call or page me [redacted]

********** -COMM. JOURNAL- ********** DATE FEB-20-1998 ***** TIME 14:32 *** P.01

MODE = MEMORY TRANSMISSION START=FEB-20 14:31 END=FEB-20 14:32

FILE NO.= 045

STN NO.	COM	ABBR NO.	STATION NAME/TEL.NO.	PAGES	DURATION
001	OK			002/002	00:00'43"

Referral/Consult

-CITAC -

********** - ***** - 202 324 0311- **********

FD-448 (Rev. 2-16-95)

FBI FACSIMILE

COVERSHEET

PRECEDENCE

- [X] Immediate
- [ ] Priority
- [ ] Routine

CLASSIFICATION

- [ ] Top Secret
- [ ] Secret
- [ ] Confidential
- [ ] Sensitive
- [X] Unclassified

Time Transmitted: _____
Sender's Initials: MJW
Number of Pages: 2
(including coversheet)

To: _____ Name of Office Date: 2/20/98

Facsimile Number: _____ Referral/Consult

Attn: _____ Name Room Telephone

From: FBI/OGC Name of Office

Subject: Detail Request Letter

Special Handling Instructions: _____

Originator's Name: _____ Telephone: _____

Originator's Facsimile Number: _____ b6 b7C

Approved: MJW

Brief Description of Communication Faxed: Per my telephone conversation

with _____ call or page me _____

(01/26/1998)

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-20-2012 BY [redacted]

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 02/23/1998

To: National Security **Attn:** SSA [redacted]
CITAC Room 11887 Ext. [redacted]

From: Newark
C-9
Contact: SA [redacted]

b6
b7C

Approved By: [redacted]

Drafted By: [redacted] :seg

Case ID #: (U) ~~(S)~~ 288-HQ-1242560 (Pending)

Title: (U) ~~(S)~~ SOLAR SUNRISE;
CITA MATTERS;
OO: HQ

Referral/Consult

Synopsis: [redacted]

(U) ~~(S)~~ ~~**Derived From : G-3**~~
~~**Declassify On: X1**~~

(U) **Administrative:** ~~(S)~~ This EC is in reference to an EC from NSD/CID to all field offices dated 02/12/1998 captioned as above.

Note: FBI Honolulu is an addressee for the enclosed material

Newark lead covered

Referral/Consult

Enclosures: [redacted]

Details: [redacted]

288-HQ-1242560-132

~~SECRET~~

1-1

To: National Security From: Newark
Re: (U) ~~(S)~~ 288-HQ-1242560, 02/23/1998

Referral/Consult

[redacted]

[redacted]

[redacted]

♦♦

DECLASSIFIED BY [redacted]
ON 09-20-2012

(12/31/1995)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY **Date:** 02/24/1998

To: FBI Headquarters **Attn:** NSD/CID/IPS
SSA [redacted]

From: Boston
Squad C-11
Contact: SA [redacted] Extension [redacted]

Approved By: [redacted]

Drafted By: [redacted]:lak

Case ID #: (U) ~~(S)~~ 288-HQ-1242560 134 (Pending)

Title: (U) ~~(S)~~ Operation Solar Sunrise
CITA Matters
OO:HQ

Synopsis: (U) Results of interview with [redacted] of Computer Services Group, Harvard University.

(U) ~~(S)~~ ~~**Classified By: 10513, C-11/Boston**~~
~~**Reason : 1.5(e)**~~
~~**Declassify On: X1**~~

Reference: (U) ~~(S)~~ 288-HQ-1242560 Serial 81

Enclosures: (U) Enclosed for Headquarters is the original and one copy of an FD-302 of [redacted] the original interview notes, a copy of [redacted]

[redacted]

Details: (U) System records from Harvard University were surrendered to SA [redacted] WFO, on February 13, 1998, at approximately 3:00 PM. The enclosed are copies of the files on the 8mm tape put into evidence at WFO. Users [redacted] and [redacted] are listed in the [redacted] as [redacted] and [redacted] Boston is still obtaining consent from all system users for a full backup of Harvard's

~~SECRET~~

To: FBI Headquarters From: Boston
Re: (U) ~~(S)~~ 288-HQ-1242560, 02/24/1998

computers.

♦♦

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-20-2012 BY [redacted]

434

January 6, 1998

Mr. Geide:

RE: INTRUSION INTO AIR FORCE SERVER

On January 6, 1998 at approximately 2:15 p.m., [redacted] Watch and Threat Analysis Unit (WTAU), received a secure call from [redacted] also of WTAU, advising that the Air Force Server had been compromised by an individual(s) who had gained access into the password file. The Air Force server is on an unclas network.

[redacted] advised that [redacted] would be contacting the WTAU with additional information as it was received. [redacted] will in turn give me a call with any additional developments. You will be kept apprised.

b6
b7C

[redacted]

1 - Mr. Geide
1 - [redacted]
(1)
MAC (3)

288-HQ-1242560

288-HQ-1242560-147

NOTES

Subject

2:15 call from [redacted] Pentagon b6 b7C
u. air force server
compromised the indiv
entn. ✓ pass &
Usclas network

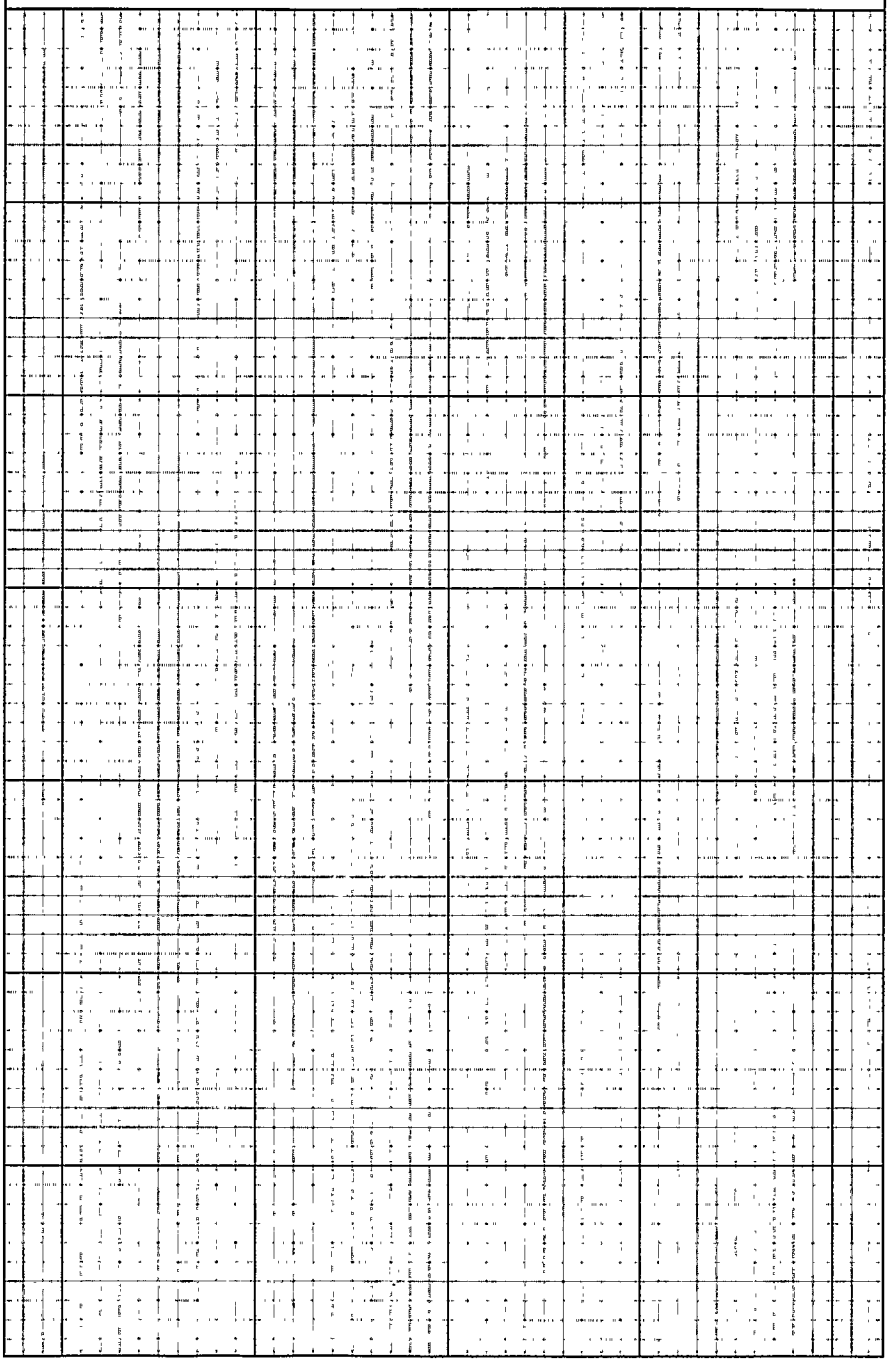
- Current sit.

located
loss // damages
theft

Printed in U.S.A. NSN #7530-01-332-1562 Reorder Part #B29

GRAPH

Project



© Productivity Plus, A Division of Franklin Quest Co.

(03/31/95)

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-20-2012 BY [redacted]

4391

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE Date: 2/20/1998

To: Director, FBI Attn: Acting Unit Chief
[redacted]

From: WFO
C-17/NVRA
Contact: SSA [redacted] b6 b7C

Approved By: [redacted]

Drafted By: [redacted]:rar

File Number(s): 288-HQ-1242560 (Pending)

Title: SOLAR SUNRISE;
CITAC MATTERS;
OO: HQ

Synopsis: Following is the status of WFO's involvement in this investigation as of 2/19/98.

Reference: EC dated 2/17/98 to Houston Division.

Details:

[redacted] U.S. NAVY - VICTIM; OO: WFO".

SA [redacted] is coordinating all investigative activity with Agents of the Naval Criminal Investigative Service (NCIS) based in both Washington, D.C. and Jacksonville, Florida. Trap & Trace/pen register order is to be signed [redacted] Results are anticipated to support a subsequent 2703 (d) order to [redacted] for [redacted] The subject's current whereabouts and employment are known. Coordination with the NCIS Agents will continue. Remote monitoring at [redacted] continuing. WFO has contacted Georgetown University, University of Virginia, and Georgia State University, and the original ISP victim/complainant in [redacted] On 2/19/98, NCIS received [redacted] from [redacted] containing [redacted] b6 b7C b7E

66-114-15-15 ENCLOSURE 140-149

(03/31/95)

FEDERAL BUREAU OF INVESTIGATION

To: WMFO From: WMFO
Re: 66-, 12/01/1995

Referral/Consult

Optical disks received from Houston. Copies will be made ASAP for AF, Navy, DISA, and [redacted] Contact has been made with IBM network management and IBM is trace routing Israeli network leg. Should know soon of monitoring ability from within US of overseas leased nets.

Analysis performed for three compromised systems: (1) Univ. California, Berkeley, (2) Andrews AFB, (3) US Naval Academy. To date, nothing significant has been identified in the most recent JID data collected for the past day or so. Observed two suspicious sites (netgate.saes.com and netdex.com). WFO has not confirmed the nexus on these sites.

Gospelcom.net not contacted due to NCIC checks revealing [redacted] Thegospel.com does not answer phone, nor do they call back when message left. Will continue to try to contact. Slip-stream.net SYSOP did not see anything unusual. They have been hacked before and do not consider this out of the norm.

On 02/13/98, Court Order served on [redacted] Legal issue with [redacted] has been addressed. Second 2703 (b) order provided to [redacted] Second order will provide additional information. Monitoring at [redacted] showed [redacted]

FERMI Labs and Oakridge National Labs report no intrusions at their sites. All traffic to/from labs is legitimate and explainable. No known connection to this case.

No further information from DISA.

[redacted] - VICTIM; OO: WFO"

SA [redacted] is addressing this matter with the assistance of the [redacted] and WFO CART. Subject's home was consensually searched for computer and computer media the evening of 2/17/98. Newark Division CART [redacted] Copy will be provided to [redacted] ASAP. Subject provided detailed interview to both FBI and [redacted] Agents. Gave no indication he was part of ongoing

b3
b6
b7C
b7E
OTHER Sealed pursuant to court order
Referral/Consult

FEDERAL BUREAU OF INVESTIGATION

To: WMFO From: WMFO
Re: 66-, 12/01/1995

investigation 288-HQ-1242560. A review of his system is under way.

Since this matter is not considered connected to the above intrusions, it will no be included in the daily briefings to CITAC.

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-25-2012 BY [redacted]

FD-448 (Rev. 6-2-97)

439

FBI FACSIMILE

COVER SHEET

PRECEDENCE

- ☐ Immediate
- ☐ Priority
- ☑ Routine

CLASSIFICATION

- ☐ Top Secret
- ☑ ~~Secret~~
- ☐ Confidential
- ☐ Sensitive
- ☐ Unclassified

Time Transmitted: 10:00 p.m.
Sender's Initials: LG
Number of Pages:
(including cover sheet)

To: FBI - Headquarters
Name of Office

Date: 2/21/98

Facsimile Number: [redacted]

Attn: [redacted]
Name Room Telephone

b6
b7C

From: FBI - Houston
Name of Office

Subject: 288-HQ-1242560

Special Handling Instructions:

Originator's Name: SSA [redacted] Telephone: [redacted]

Originator's Facsimile Number: [redacted]

Approved:

Brief Description of Communication Faxed: [redacted]-HQ-1[redacted]-150

1

WARNING

Information attached to the cover sheet is U.S. Government Property. If you are not the intended recipient of this information, disclosure, reproduction, distribution, or use of this information is prohibited (18.USC, § 641). Please notify the originator or local FBI Office immediately to arrange for proper disposition.

FD-448 (Rev. 6-2-97)

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-20-2012 BY [redacted]

4-4

FBI FACSIMILE

COVER SHEET

PRECEDENCE

- ☐ Immediate
- ☐ Priority
- ☑ Routine

CLASSIFICATION

- ☐ Top Secret
- ☑ ~~Secret~~
- ☐ Confidential
- ☐ Sensitive
- ☐ Unclassified

Time Transmitted: 7:10 & 7:55 p.m.
Sender's Initials: SA
Number of Pages: 16
(including cover sheet)

To: FBI Headquarters Date: 2/21/98
Name of Office

Facsimile Number: [redacted]

Attn: [redacted]
Name Room Telephone

From: FBI - Houston
Name of Office

b6
b7C

Subject:

Special Handling Instructions:

Originator's Name: SA [redacted] Telephone: [redacted]

Originator's Facsimile Number [redacted]

Approved:

Brief Description of Communication Faxed: 3-116-134250-151

288-HQ-1242560

1

WARNING

Information attached to the cover sheet is U.S. Government Property. If you are not the intended recipient of this information, disclosure, reproduction, distribution, or use of this information is prohibited (18.USC, § 641). Please notify the originator or local FBI Office immediately to arrange for proper disposition.

TOTAL P.01

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-20-2012 BY [redacted]

431

February 25, 1998

Director Freeh:

RE: SOLAR SUNRISE;
CITA MATTER
OO: HQ

The captioned investigation involves intrusions into computers within the United States which began around January 13, 1998, and continuing to date. The computers which have been compromised are computers belonging to the United States Air Force, located at Andrews AFB, Maryland, Kirkland AFB, New Mexico, Columbus AFB, Ohio, Lackland AFB, Texas, Gunter AFB, Alabama, and Channel Island, ANGS, California; computers belonging to the United States Navy, located at the United States Naval Academy in Annapolis, Maryland, Pearl Harbor, Hawaii, and computers belonging to the United States Marine Corps Base, Camp Butler, Okinawa, Japan.

Most of the compromised computers are Domain Name Servers (DNS), i.e. fbi.gov. DNS systems are responsible for translating domain names into their respective Internet Protocol(IP) addresses. IP addresses are essential for Internet computer communications. Intrusions into such computers have the potential to disrupt the mission of the U.S. military throughout the world.

From logs obtained from various Internet service providers and universities, investigators have determined that the intruder(s) originated from SONIC.NET an Internet service provider, in Santa Clara, California. Court Orders served on [redacted] revealed that [redacted]

b3
OTHER Sealed pursuant to court order

On February 9, 1998, the Massachusetts Institute of Technology (MIT) [redacted] contacted SONIC.NET regarding a computer intrusion. [redacted] at MIT, stated that someone had intruded their system from SONIC.NET and provided the Internet Protocol (IP) address. The IP address is known to be associated with [redacted] DOB [redacted]

b6
b7C

On February 16, 1998, electronic surveillance was initiated by the FBI on the user account [redacted] The Order was signed on [redacted]

b3
b6
b7C
OTHER Sealed Pursuant to court order [redacted]

288-HQ-1242520-152

288-HQ-1242520

[redacted] b6 b7C
[redacted] are subjects of this investigation and are associates.

Another site identified as a "launching point" for the intrusions is Maroon.com, a web publisher located at College Station, Texas. [redacted] and a search warrant has been served for [redacted] b7E

A trap and trace Order was signed and executed on [redacted] A trap and trace Order is already in place for [redacted] b3

On [redacted] FBI SF initiated a Title III Order on [redacted] A Title III Order is now being pursued for [redacted] Additionally, [redacted] are also being obtain for each subject. b3 b7E

To date, 15 court orders have been served to include one Title III and two consensual monitoring sites. Two more orders are presently being obtained to include another Title III.

This matter is being coordinated with [redacted] DOJ, DOD, and others as new developments arise.

Referral/Consult

K.M. Geide

NOT APPROPRIATE FOR DISSEMINATION TO THE PUBLIC

1 - [redacted]
1 -
1 -
1 -
1 -
1 -
1 -
1 -
APM:apm (11)

1 - Mr. Geide
1 - [redacted] b6 b7C
1 -

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-20-2012 BY [redacted]

(03/31/95)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE Date: 2/24/1998

To: Director, FBI Attn: Acting Unit Chief
[redacted]

From: WFO
C-17/NVRA
Contact: SSA [redacted]

b6
b7C

Approved By: [redacted]

Drafted By: [redacted]:rar

File Number(s): 288-HQ-1242560 (Pending) -154

Title: SOLAR SUNRISE;
CITAC MATTERS;
OO: HQ

Synopsis: Following is the status of WFO's involvement in this investigation as of 2/24/98.

Reference: EC dated 2/17/98 to Houston Division.

Details:

[redacted] U.S. NAVY - VICTIM; OO: WFO".

SA [redacted] is coordinating all investigative activity with Agents of the Naval Criminal Investigative Service (NCIS) based in both Washington, D.C. and Jacksonville, Florida. Trap & Trace/pen register installation still problematic. The subject's current whereabouts and employment are known. Coordination with the NCIS Agents will continue. Remote monitoring at [redacted] continuing. Intrusions through IAP.NET into MIT will be addressed by NCIS only.

b3
b6
b7C
b7E

288-HQ-1242560 "SOLAR SUNRISE: CITAC MATTERS: OO: HQ"

Copies of [redacted] copied at FBIHQ CART were blank. Original evidence in the hands of [redacted] SSA [redacted] is following through to resolve. [redacted] related to the [redacted] account to be copied tomorrow by FBIHQ CART per CITAC. Access to account originated from the University of Phoenix, "online.uops.fo.uophx.edu." WFO will follow through.

b6
b7C
b7E
Referral/Consult

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-20-2012 BY [redacted]

(12/31/1995)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY **Date:** 02/23/1998

To: NSD/CID **Attn:** CITAC/Room 11887
SSA [redacted]

From: Albuquerque
Squad 8
Contact: SA [redacted]

b6
b7C

Approved By: [redacted] 2/23/98

Drafted By: [redacted] :cmh

Case ID #: (U) ~~(S)~~ 288-HQ-1242560 (Pending) 156

Title: (U) ~~(S)~~ SOLAR SUNRISE;
CITA MATTERS;
OO: HQ;

Synopsis: (U) Lead Covered.

(U) ~~(S)~~ ~~**Derived From : Single Source Document**~~
~~**See Classification Authority Reference Section.**~~
~~**Declassify On: 02/12/2008**~~

(U) ~~**Classification Authority Reference:**~~ ~~(S)~~ ~~See Reference Section;~~ Classified By: 4511, ~~CITAC/D5; Reason: 1.5(c);~~ Declassify On: 02~~/12/2008~~

Reference: (U) ~~(S)~~ 288-HQ-1242560 Serial 52 Referral/Consult

~~SECRET~~

To: NSD/CID From: Albuquerque
Re: (U) ~~(S)~~ 288-HQ-1242560, 02/23/1998

Referral/Consult

[redacted]

[redacted]

(U) ~~(S)~~ Las Cruces RA and Roswell RA have been asked to forward any information concerning possible intrusions at Holloman AFB and Cannon AFB respectively. No further investigation remains at Albuquerque.

♦♦

DECLASSIFIED BY [redacted]
ON 09-21-2012

(12/31/1995)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY **Date:** 02/23/1998

To: Albuquerque **Attn:** Las Cruces RA
Roswell RA
NSD/CID **Attn:** CITAC/Room 11887
SSA [redacted]

From: Albuquerque
Squad 8
Contact: SA [redacted] b6 b7C

Approved By: [redacted] 2/23/98

Drafted By: [redacted] :cmh

Case ID #: (U) ~~(S)~~ 288-HQ-1242560-158 (Pending)

Title: (U) ~~(S)~~ SOLAR SUNRISE;
CITA MATTERS;
OO: HQ;

Synopsis: (U) To set leads at Las Cruces RA and Roswell RA.

(U) ~~(S)~~ ~~**Derived From : Single Source Document**~~
~~**See Classification Authority Reference Section.**~~
~~**Declassify On: 02/12/2008**~~

(U) ~~**Classification Authority Reference:** (S) See Reference Section;~~
~~Classified By: 4511, CITAC/D5; Reason: 1.5(c); Declassify On: 02/12/2008~~

Reference: (U) ~~(S)~~ 288-HQ-1242560 Serial 52

Details: (U) ~~(S)~~ On 02/01/1998, the Department of Defense (DOD) began detecting computer intrusions into its unclassified computer systems at various facilities in the United States. These intrusions are ongoing. At least 11 DOD systems are known to have been compromised and recovery procedures have been initiated. The intruder appears to have targeted domain name servers and obtained root status via exploitation of the "statd" vulnerability in the Solaris 2.4 operating system. Hacker tools imported from a University of Maryland site were used to gain entry. The intruder installed a sniffer program and then closed the vulnerability by transferring a patch from the University of North Carolina. A "backdoor" was created to allow the intruder reentry to the system.

~~SECRET~~

To: Albuquerque From: Albuquerque
Re: (U) ~~(S)~~ 288-HQ-1242560, 02/23/1998

(U) ~~(S)~~ Intrusions, or intrusion attempts, were detected at Andrews Air Force Base (AFB), Columbus AFB, Kirkland AFB, Maxwell AFB (Gunter Annex), Kelly AFB, Lackland AFB, Shaw AFB, MacDill AFB, Naval Station Pearl Harbor, and an Okinawa Marine Corps Base.

(U) ~~(S)~~ Numerous university computer sites in the U.S. appear to have been exploited in a similar fashion. Internet service providers near those universities also appear to have been exploited to access, or attempt to access, DOD computer networks.

(U) ~~(S)~~ In the referenced communication, FBIHQ requested all field offices expeditiously contact all logical sources for any information pertaining to intrusions into Air Force domain name servers using the "statd" exploit on Solaris 2.4 operating systems.

To: Albuquerque From: Albuquerque
Re: (U) ~~(S)~~ 288-HQ-1242560, 02/23/1998

LEAD (s):

Set Lead 1:

LAS CRUCES RA

AT ALAMOGORDO, NM

(U) ~~(S)~~ Expeditiously contact the Office of Special Investigations (OSI) at Holloman AFB, ALAMOGORDO, New Mexico, telephone number [redacted] or [redacted] Determine if they have any information pertaining to intrusions into Air Force domain name servers using the "statd" exploit on Solaris 2.4 operating systems. Respond expeditiously with positive results to SSA [redacted] or SSA [redacted] FBIHQ, NSD/CID, CITAC, telephone number [redacted]

b6
b7C

Set Lead 2:

ROSWELL RA

AT CLOVIS, NM

(U) ~~(S)~~ Expeditiously contact the Office of Special Investigations (OSI) at Cannon AFB, Clovis, New Mexico, telephone number [redacted] or [redacted] Determine if they have any information pertaining to intrusions into Air Force domain name servers using the "statd" exploit on Solaris 2.4 operating systems. Respond expeditiously with positive results to SSA [redacted] or SSA [redacted] FBIHQ, NSD/CID, CITAC, telephone number [redacted]

b6
b7C

♦♦

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-21-2012 BY [redacted]

(01/26/1998)

Forwarded to HQ

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY **Date:** 02/23/1998

To: ✓WFO **Attn:** C-17
[redacted]

From: Kansas City
Squad 4
Contact: IA [redacted]

b6
b7C

Approved By: [redacted]

Drafted By: [redacted] :ajg

Case ID #: 288-HQ-1242560 b9 (Pending)

Title: UNSUB(S):
UNITED STATES AIR FORCE;
ET AL-VICTIM;
CITA

b3
OTHER Sealed Pursuant to Court Order

Synopsis: Court orders delivered to [redacted]

Reference: 288-HQ-1242560 Serial 19
288-HQ-1242560 Serial 8

Details: On 12/13/98, [redacted] accepted delivery of court order, dated [redacted] and court order, dated [redacted]

[redacted] advised they would comply with the court order.

All leads assigned to KC have been completed.

♦♦

uploaded 2/27/98 / KC

DHG 3/23/98

(12/31/1995)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-21-2012 BY [redacted]

434

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 02/26/1998

To: National Security **Attn:** [redacted]

From: Acting Unit Chief [redacted]
CITAC/CIU/Room 11887
Contact: SSA [redacted] b6 b7C

Approved By: Geide Kenneth M KMG

Drafted By: [redacted] :skl

Case ID #: 288-HQ-1242560 -1163 (Pending)

Title: SOLAR SUNRISE
CITA MATTERS

Synopsis: Document equipment requests for captioned case.

Details: Captioned case involves intrusions into various military, commercial, and educational computer networks. Due to the large amounts of data received from intercepts, consensuals, and log requests, San Francisco and Houston divisions requested various computer equipment to be sent to them in an expeditious manner. The equipment sent to them is to be deducted from any requests for equipment from the field. Also, [redacted] is going to [redacted]

[redacted] b6 b7C b7E

The following has been requested by the writer to date:

1. One laptop to San Francisco SSA [redacted]
2. One laptop and two extra hard drives to SA [redacted] Houston.
3. One extra laptop hard drive for [redacted]

The writer appreciates the expeditious attention given to these requests by CS [redacted] STAU.

♦♦

Initialed by [redacted] 2/25/98

Page 88 ~ Referral/Direct;
Page 89 ~ Referral/Direct;
Page 90 ~ Referral/Direct;
Page 91 ~ Referral/Direct;
Page 92 ~ Referral/Direct;
Page 93 ~ Referral/Direct;
Page 94 ~ Referral/Direct;
Page 95 ~ Referral/Direct;
Page 96 ~ Referral/Direct;
Page 97 ~ Referral/Direct;
Page 98 ~ Referral/Direct;
Page 99 ~ Referral/Direct;
Page 100 ~ Referral/Direct;
Page 101 ~ Referral/Direct;
Page 102 ~ Referral/Direct;
Page 103 ~ Referral/Direct;
Page 104 ~ Referral/Direct;
Page 105 ~ Referral/Direct;
Page 106 ~ Referral/Direct;
Page 107 ~ Referral/Direct;
Page 108 ~ Referral/Direct;
Page 109 ~ Referral/Direct;
Page 110 ~ Referral/Direct;
Page 111 ~ Referral/Direct;
Page 112 ~ Referral/Direct;
Page 113 ~ Referral/Direct;
Page 114 ~ Referral/Direct;
Page 115 ~ Referral/Direct;
Page 116 ~ Referral/Direct;
Page 117 ~ Referral/Direct;
Page 118 ~ Referral/Direct;
Page 119 ~ Referral/Direct;
Page 120 ~ Referral/Direct;
Page 121 ~ Referral/Direct;
Page 122 ~ Referral/Direct;
Page 123 ~ Referral/Direct;
Page 124 ~ Referral/Direct;
Page 125 ~ Referral/Direct;
Page 126 ~ Referral/Direct;
Page 127 ~ Referral/Direct;
Page 128 ~ Referral/Direct;
Page 129 ~ Referral/Direct;
Page 130 ~ Referral/Direct;
Page 131 ~ Referral/Direct;
Page 132 ~ Referral/Direct;
Page 133 ~ Referral/Direct;
Page 134 ~ Referral/Direct;
Page 135 ~ Referral/Direct;
Page 136 ~ Referral/Direct;
Page 137 ~ Referral/Direct;
Page 138 ~ Referral/Direct;
Page 139 ~ Referral/Direct;
Page 140 ~ Referral/Direct;
Page 141 ~ Referral/Direct;
Page 142 ~ Referral/Direct;
Page 143 ~ Referral/Direct;
Page 144 ~ Referral/Direct;
Page 145 ~ Referral/Direct;
Page 146 ~ Referral/Direct;
Page 147 ~ Referral/Direct;
Page 148 ~ Referral/Direct;
Page 149 ~ Referral/Direct;
Page 150 ~ Referral/Direct;
Page 151 ~ Referral/Direct;
Page 152 ~ Referral/Direct;
Page 153 ~ Referral/Direct;
Page 154 ~ Referral/Direct;
Page 155 ~ Referral/Direct;
Page 156 ~ Referral/Direct;
Page 157 ~ Referral/Direct;
Page 158 ~ Referral/Direct;
Page 159 ~ Referral/Direct;
Page 160 ~ Referral/Direct;